

**BakerHostetler**

RECEIVED  
OCT 21 2020  
CONSUMER PROTECTION

**Baker & Hostetler LLP**

11601 Wilshire Boulevard  
Suite 1400  
Los Angeles, CA 90025-0509  
T 310.820.8800  
F 310.820.8859  
www.bakerlaw.com

M. Scott Koller  
direct dial: 310.979.8427  
mskoller@bakerlaw.com

October 20, 2020

**VIA OVERNIGHT MAIL**

Attorney General Gordon MacDonald  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

*Re: Incident Notification*

Dear Sir or Madam:

We are writing on behalf of our client, the City of Torrance, California. (the “City”), to notify you of a security incident.

On March 1, 2020, the City identified a ransomware infection in its network. Upon learning this, the City notified law enforcement, retained Baker & Hostetler, LLP (“BakerHostetler”) to provide legal advice and assistance investigating and responding to the incident, and BakerHostetler, on behalf of the City, engaged cybersecurity professionals to conduct a forensic investigation to allow BakerHostetler to provide legal advice to the City.

While the investigation was still ongoing, the City learned that someone claiming responsibility for the ransomware incident had posted data to the internet that was purported to be from the City. On April 28, 2020, the City decided to notify all of its employees, while also continuing to review the data posted on the internet in the event that non-employee information was contained in the data as well. On May 8, 2020, the City determined that some data posted on the internet included individual names, Social Security numbers, driver’s license numbers or state identification numbers, and financial account information of some non-City employees.

After the initial notices were mailed, the review of data continued to identify additional individuals whose information was contained in the data. On August 4, 2020, the review

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Dallas Denver Houston  
Los Angeles New York Orlando Philadelphia San Francisco Seattle Washington, DC

concluded. However, addresses for many of the individuals were not located during the review process. The City then conducted additional research to locate addresses for the affected individuals. That process concluded at the end of September. The City notified one New Hampshire resident of this incident in the second round of notifications.

On October 13, 2020, the City mailed notification letters via United States Postal Service First Class Mail to the one New Hampshire resident in accordance with N.H. Rev. Stat. Ann. § 359-C:20.<sup>1</sup> A sample copy of the notification letter is enclosed. The City has established a dedicated call center where all individuals may obtain more information regarding the incident. Notification of this incident is being provided as quickly as possible, following the completion of the investigation, which was performed without unreasonable delay, despite significant challenges faced by the City due to the COVID-19 pandemic.

To help prevent a similar incident from occurring in the future, the City is implementing additional technical safeguards and reconfiguring some network appliances. In addition, the City continues to cooperate with law enforcement to investigate this incident.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



M. Scott Koller  
Partner

Enclosure.

---

<sup>1</sup> This report is not and does not constitute a waiver of the City's objection that New Hampshire lacks personal jurisdiction over it related to any claims that may arise from this incident.



CITY OF  
TORRANCE

Return Mail Processing  
PO Box 589  
Claysburg, PA 16625-0589

October 9, 2020

F8736-L04-0000004 P001 T00001 \*\*\*\*\*MIXED AADC 159



SAMPLE A SAMPLE - L04 CM  
APT 123  
123 ANY ST  
ANYTOWN, US 12345-6789



Dear Sample A Sample:

The City of Torrance understands the importance and takes very seriously its responsibility to protect personal information. We are writing to inform you of a recent cybersecurity incident that may have involved some of your information. This notice explains the incident, measures we have taken and steps you can take in response.

On March 1, 2020, the City announced that it had experienced a cybersecurity incident that affected some of its computer systems. During the course of its investigation, the City learned that some data that was taken during the incident was accessible on the internet. On August 4, 2020, we determined that one or more documents that were compromised in this incident may contain your name [Extra 1].

The City of Torrance is taking this incident very seriously. As a precaution, we are offering you a complimentary one-year membership in Experian® IdentityWorks<sup>SM</sup> Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score.

We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. For more information on IdentityWorks Credit 3B, including instructions on how to activate your complimentary membership and some additional steps you can take to help protect yourself, please see the additional information provided with this letter.

We sincerely regret any concern or inconvenience caused by this incident. Information security enhancements were deployed immediately and additional protections are being implemented. If you have any questions, please call (866) 581-1076 Monday through Friday from 6 a.m. to 8 p.m. PST, and Saturday and Sunday from 8 a.m. to 5 p.m. PST.

Sincerely,

Aram Chaparyan  
City Manager  
City of Torrance  
3031 Torrance Blvd.  
Torrance, CA 90503

0000004



F8736-L04

## Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **December 31, 2020** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(866) 581-1076** by **December 31, 2020**. Be prepared to provide engagement number **DB22699** as proof of eligibility for the identity restoration services by Experian.

### ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **(866) 581-1076**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

\* Offline members will be eligible to call for additional reports quarterly after enrolling.

\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

## **ADDITIONAL STEPS YOU CAN TAKE**

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

### ***Fraud Alerts and Credit or Security Freezes:***

**Fraud Alerts:** There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

**Credit or Security Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

*How do I place a freeze on my credit reports?* There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

0000004



*How do I lift a freeze?* A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

**Additional information for residents of the following states:**

**Maryland:** You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, [www.oag.state.md.us](http://www.oag.state.md.us)

**Massachusetts:** Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, [www.mass.gov/ago/contact-us.html](http://www.mass.gov/ago/contact-us.html)

**New York:** You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

**North Carolina:** You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov)

**Rhode Island:** This incident involves one individual in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, [www.riag.ri.gov](http://www.riag.ri.gov)

**West Virginia:** You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

**A Summary of Your Rights Under the Fair Credit Reporting Act:** The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to [www.consumerfinance.gov/learnmore](http://www.consumerfinance.gov/learnmore) or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.

- You may limit “prescreened” offers of credit and insurance you get based on information in your credit report.
- You have a right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.



